

Introduction

There are many things to consider when planning a wireless implementation in your district such as which technologies to use, coverage, standalone or centrally controlled, security, etc. This guide will address the considerations necessary to implement a healthy and secure wireless network.

I. Site Survey

A site survey will help determine the placement of Access Points (AP) in a building. AP Placement is affected by the materials used in the building structure. The size of the signal concentration (cell) for each AP can vary due to these materials. Correct placement is critical to provide the required signal concentration necessary for the applications that will be run over the wireless network.

A. There are 3 AP deployments to consider when requesting a site survey: data only, voice and RFID (Radio-Frequency Identification) tags.

1. If the wireless network will only be used to augment the wired data network, this is considered data only and will require the least amount of signal saturation (cell).
2. VoIP over a wireless network requires a denser signal saturation to insure call quality. This requires a more dense population of Access Points with overlapping cells.
3. RFID tags are used to track the location of devices or people. RFID tags require a very dense wireless signal saturation since the signal from the device cannot be lost at any time.

B. A thorough assessment of the network infrastructure should be conducted in conjunction with a wireless assessment to determine the number of PoE ports available to accommodate the access points. (Please refer to **Section VI. Infrastructure** for more information).

C. Conducting a site survey can be done through a vendor, by using software or manually.

1. There are many vendors that conduct site surveys however, these can be very expensive. Software products like AirMagnet or Ekahau can also be used to conduct wireless surveys. These products have a hefty price tag, a steep learning curve, and are time intensive to use. They yield very accurate results since they take into account everything such as building floor plans, building materials, and things in the environment that can interfere with the wireless signal.
2. A manual survey can be accomplished by setting up Access Points in buildings and recording signal strengths. This will help with determining the placement and number of Access Points. This method should only be used for data only implementations.
3. Consider "iDevices" (iPad, iPod etc..) as the weakest transmitted power devices on the WLAN and plan according to these radio strengths which could increase the number of access points needed.

D. When planning new wireless deployments or infrastructure projects, planning should take into consideration the coming 802.11ac standard and make sure the new infrastructure is able to support it.

E. Post Install Survey should be conducted to determine adequate coverage in the wireless network, to test connectivity and application speeds.

II. Applications and Users

A. The applications that will be used on your wireless network need to be a consideration.

1. Some applications require more network resources and may have issues running over a wireless network. It may be necessary to check with the technical support of a software vendor if you are not sure. Older versions of software may also require upgrades to run wirelessly.
2. User surveys are often helpful to determine applications.

B. Computer labs should be given special consideration. Wireless is a shared media and throughput is affected by the number of users on a given access point. Consider that in a wireless environment only one device at a time can talk to the AP. Coverage for the lab may be accomplished by placing a single access point in the room; however in a lab with 20 or more wireless nodes, multiple access points would be necessary.

III. Hardware Considerations

A. There are 2 types of technologies to consider, standalone and centrally controlled.

1. A standalone (**Autonomous**) implementation uses individually controlled access points. Each access point must be configured separately and troubleshooting a problem can be very tedious. On the surface it could be considered a more cost effective method for managing a wireless network. However, as the number of AP's increases the more administratively intensive the wireless network becomes.
2. Centrally controlled implementations using a Wireless LAN Controller should seriously be considered with any wireless deployment of any significant size. All access points are configured and managed through the controller which simplifies deployment and troubleshooting. This solution offers the capability of running multiple controllers. Wireless Control System (WCS) software can be used to manage multiple controllers and access points.

B. There are 2 frequencies to consider for your wireless 2.4 GHZ and 5GHZ.

1. Wireless signals operating in the 2.4 GHZ range are susceptible to RF interference from other devices such as portable phones and microwaves. The interfering RF signals degrade the performance of a wireless network by periodically blocking users and access points from

accessing the shared air medium. The wireless standards that operate in this frequency range are 802.11b, 802.11g, and 802.11n.

a. Due to the age and reduced speed of the standard (11 Mbps), it is recommended to avoid using and eliminate 802.11b in your environment whenever possible.

b. 802.11G operates at a maximum speed 54 Mbps and is widely used. Newer deployments should consider 802.11a or n

2. Wireless signals operating in the 5 GHz are above most local interference and provide better signal quality. As frequency increases, range generally decreases. As a result, 5 GHz systems, based only on frequency, may have less range than ones operating in the 2.4 GHz band. This means that the selection of 5 GHz spectrum could require a greater number of access points, which results in higher costs. The wireless standards that operate in this frequency range are 802.11a, 802.11n, and 802.11 ac.

a. 802.11a

1. Supports a maximum bandwidth of 54 Mbps
2. The range of an 802.11a signal is limited to the 5 GHz frequency.
3. Brick walls and other obstructions affect 802.11a wireless networks to a greater degree than they do comparable 802.11b/g networks.
4. Higher cost than that of 802.11b and 802.11g

b. 802.11n

1. 802.11n supports both 2.4 GHz and 5 GHz clients.
2. Is configurable on the controller to allow the wireless client to connect at a maximum speed of 300Mbps.

c. 802.11ac

1. Ratified in 2012
2. Also known as: VHT (Very High Throughput)
3. Has no support for 802.11b/g.
4. Based only on the 802.11a radio spectrum and supports only 5 GHz clients.
5. It increases 802.11n bandwidth speeds to over 1 Gbps,

3. 802.11n and 802.11ac access points should have Gigabit access to the LAN although they will negotiate to 100 Mbps if that is what is available. It is recommended that tri-speed (10/100/1000) PoE switches be used to connect these access points to the LAN.

4. Purchases of any new wireless equipment should follow the standard of Dual Radio 802.11a/b/g/n wireless technology.

IV. Consumer and Commercial Grade Wireless Networks

A. There are 2 different grades of wireless hardware to consider, consumer grade and commercial grade.

1. Consumer Grade - Standalone only (\$50 - \$150)

- a.** Brands Include: Linksys, D-Link, Netgear, Apple, etc...
- b.** Consumer grade access points have lower memory and processors. They are designed for a small number of users connecting in a home or small business environment. Having many clients on a consumer grade access point would overwhelm it causing unacceptable response times.
- c.** The radio power is typically low, designed only to cover areas equivalent to the average house and minimize interference with other devices like cordless phones.
- d.** The controls in the access point are bare-bones which would not allow for enhanced security settings that enterprise networks require.
- e.** The hardware is also limited. The majority of the antennas are permanently attached and cannot be removed or changed.
- f.** Technical support for these devices tends to be minimal.

2. Commercial Grade - Standalone or Centrally Managed (\$400 - \$800).

- a.** Brands include: Cisco, Aruba, Meru, Xirrus, Proxim, Avaya (Trapeze) . . .
- b.** If purchased as standalone, these can be added to a centrally managed system.
- c.** Commercial grade wireless networking systems have more powerful processors and more memory, enabling them to support larger number of clients.
- d.** The radio power can be adjusted to cover a smaller cell around the access point. This provides a higher density for applications such VoIP over wireless. The radios can also be set to automatically increase power to cover a failed access point.
- e.** Software is available to give a global view of the wireless network, providing information on each access point, rogue access points (unauthorized access points), and all connected clients.
- f.** From a security perspective, access points can be set to destructively interfere with rogue access points, making them useless and disabling any clients that connect to it, thereby keeping all users on only the authorized access points.
- g.** The access points can be setup to force users to authenticate through a central server such as RADIUS.
- h.** Some models have removable radio modules allowing upgrades to accommodate new standards or more powerful radios.
- i.** Certain access points have external antennas that can be changed to provide appropriate coverage.
- j.** Through a maintenance contract technical support is available and able to assist in complex technical problems.

V. Security

There are two parts to securing the data on your wireless network, authentication to the access point with encryption and network authentication. Data encryption is necessary to prevent a person from intercepting your data from the airways and having it available in clear text. The access point can be run in an open state without encryption or authentication but this is not recommended.

A. Wireless authentication permits access to the access point and encrypts the data. The encryption methods are WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and WPA2.

1. WEP was originally intended to give you the same or similar level of security as on a wired network but it turns out that it does not. WEP, has serious security weaknesses and has been superseded by WPA. WEP is not difficult to crack, and using it reduces performance slightly.

2. Just as WPA replaced WEP, WPA2 has replaced WPA as the most current security protocol. WPA2 implements the latest security standards, including "government-grade" data encryption. Since 2006, all Wi-Fi CERTIFIED products must use WPA2 security.

B. Network authentication requires the use of an external server such as RADIUS or a network appliance such as the Cisco Access Control Server. The user first connects to the access point, then if applicable to the controller, and then is authenticated against a user database such as Active Directory. A computer name may also be checked against a database to add to the security process. An IP address is not issued until the authentication process is complete.

VI. Infrastructure

A. The wired infrastructure is often overlooked when implementing a wireless network. Consider that the AP must connect to the wired network and is passing data from multiple machines.

B. Older wiring to patch panels or switches may intermittently cause retransmissions of data to or from a PC or laptop. This may appear as an occasional slow response on a wired network. With wireless communications the result would show as an unstable and unreliable wireless network. Consider the age of your infrastructure and running new lines to your Access Points.

C. Switching hardware must also be a consideration in a wireless deployment.

A. Power over Ethernet (PoE) has come down in cost. it should be considered for all closets in infrastructure capital projects to accommodate for AP's and other devices such as cameras and even Virtual Desktop Infrastructure (VDI). Determine the max watt output per switch and take into consideration the higher heat output of POE switches.

B. Power over Ethernet Midspan devices - These switch-like power injector devices can be purchased to expand the current infrastructure to add power.

D. Access points can be powered with Power over Ethernet (PoE) switches or with external power supplies. PoE switches should be considered whenever possible for larger wireless deployments.

1. Check with the Vendor to verify the power requirements of the access points.

2. Some 802.11n access points require up to 30W of power consumption with PoE. There are 2 standards that address this, 80211.af and 80211.at.

- a. 80211.af is the original standard and was approved for 15W per port over Cat 5 cabling.

- b. 80211.at is a newer standard to address the need for high powered devices requiring 30W per port.

E. Since the 802.11n AP's are capable of over 300 Mbps throughput and 802.11ac are capable of up to a 1 Gbps throughput, these AP's should be connected to a gigabit switch port.

VII. Guest Access

Providing wireless Internet access to guests (contractors, visitors, staff and students who bring their own devices etc.) can help improve communication, productivity, and allow access to necessary resources while denying access to the internal network. For example, visitors attending meetings may need Internet access for webmail or VPN access to obtain files for a presentation. Thoughtful consideration should be given to developing a policy that addresses how wireless guest users will access the wireless network, what wireless devices will be allowed to access the wireless network, and what locations on the wireless network will allow guest access, such as conference rooms and offices.

A. In most implementations, access to a guest network can be limited to areas such as conference rooms, or office areas. However, it may be extended to include any or all of the wireless coverage.

B. A Guest VLAN can be configured to keep guest users from being able to access corporate network resources. With the Guest VLAN, guest traffic can be tagged so that any Guest VLAN traffic is sent straight to the firewall/web content filter. In this manner, guests obtain only filtered Internet access, even though their traffic is traversing the private network.

C. There are four methods for controlling access to a wireless network:

1. Open

a. Anyone can connect to an open network and it eliminates the need for configuration on guest machines. The downside is that unwanted guests (e.g., neighboring businesses) can also connect to the open network freely.

b. Wireless is a shared media and throughput is affected by the number of users connected to a given access point. Since open access allows any wireless device to access the wireless network, a single AP may become overwhelmed through unmanaged wireless devices such as iPod Touches, etc.

2. Pre-shared keys (PSK)

A pre-shared key (PSK) is used to encrypt traffic sent between a client device and a wireless AP. Only users with the correct PSK can send and receive data. The key is “pre-shared” because it must be manually configured before the client can associate to the wireless network. PSK dramatically improves protection over WEP. It is designed for home or small network use due to the administrative overhead. Enterprise environments are encouraged to move towards WPA2 Enterprise w/AES which requires 802.1x authentication.

3. Authentication

Individual user authentication provides more secure access control than either an open network or a PSK encrypted network.

a. For guest access, the splash page login is recommended because it requires no client-side configuration. The splash page simply displays within the guest user’s browser and provides instructions to the user on how acquire login credentials.

b. This implementation will vary with the chosen platform. For example, the Cisco wireless controller allows a “Lobby Administrator” account to be created. The Lobby Administrator can assign usernames and passwords on the guest wireless network. This can be a tedious task for someone to administer but prevents unwanted devices from accessing the wireless network.

c. 802.1x Authentication –

Authentication means making sure that something is what it claims to be. The purpose of 802.1x is to accept or reject users who want full access to a network using 802.1x. It is a security protocol that works with 802.11 wireless networks.

The main parts of 802.1x Authentication are:

1. A supplicant - a client end user which wants to be authenticated.
2. An authenticator (an access point or a switch), which is a “go between”, acting as proxy for the end user, and restricting the end user’s communication with the authentication server.

3. A Network Policy Server (NPS), usually a RADIUS server, decides whether to accept the end user's request for full network access. The Radius Server validates user credentials to eDirectory, Active Directory, or OpenDir. Microsoft Servers have the ability to combine the Radius Server with Active Directory to make authentication seamless.

4. MAC Address Filtering

Wireless devices can be allowed or denied on your network according to their MAC addresses. However, this method is one of the least secure and is not recommended because MAC addresses can be easily spoofed which would allow unwanted devices to access your network. In addition maintaining a list of MAC addresses for guests' devices is cumbersome and time consuming.

D. As mentioned earlier, personal mobile devices using a guest network can have an adverse effect on AP throughput and Internet bandwidth. These devices can be restricted from the network or have bandwidth limits imposed.

1. One method of restricting personal mobile devices is through the use of a RADIUS server. The Radius Server queries the Active Directory or LDAP server database. By configuring the authentication to accept only valid machine names instead of login credentials, any unknown devices on the wireless LAN are not allowed to connect.
2. If personal mobile devices are allowed to access the wireless network bandwidth limitations may be placed on these devices using a packet shaping device.

VIII. Bring Your Own Device (BYOD) -

The use of personal mobile devices in the workplace is ever increasing. Allowing these devices into your network creates concerns of how to create a secure and productive mobile environment. Each network will present its own unique challenges but there are some general things to consider.

A. Policies - To effectively leverage the management of personal mobile devices policies must be determined and put into place prior to implementation. There should be consideration to given to any Terms and Conditions or Acceptable Usage Agreements to be accepted before login.

1. Compliance - Are there any regulations, such as HIPAA, that govern data that needs to be protected?

2. Security - What security measures (antivirus, password protection) must be taken on the network to allow access to certain resources?

3. Privacy - What data is being collected from personal user devices?

B. Devices - What mobile devices will be supported? Only certain devices or whatever the user wants? (Reference iDevices section).

C. Applications - What applications on the personal device should be prohibited if any?

D. Lost devices - If a personal device is lost or stolen, consider having a policy to ensure it is reported immediately. The device could be wiped (completely erased) through any mobile device management application such as Exchange.

E. Additional Equipment - Will additional access points need to be added to certain areas to handle the increased number of personal mobile devices?

F. Equipment/Application Considerations – Network Access Control (NAC) and Mobile Device Management (MDM) can assist with many of the security and management concerns mentioned above.

1. Network Access Control (NAC) is normally an appliance based solution that attempts to unify network security on all endpoints (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.
2. Mobile Device Management (MDM) such as AirWatch, Good Technology, MobileIron, and Zenprise enables you to manage large-scale deployments of mobile devices. MDM provides the following:
 - a. the ability to quickly enroll devices in your enterprise environment,
 - b. configure and update device settings over-the-air
 - c. enforce security policies and compliance
 - d. secure mobile access to corporate resources
 - e. and remotely lock and wipe managed devices.
 - f. allows management of a diverse fleet of Android, Apple, BlackBerry, Mac OS X, Symbian, and Windows devices in a single console.